ERIC A. GROVER (SBN 136080)
eric.grover@kellergrover.com
RACHAEL G. JUNG (SBN 239323)
rachael.jung@kellergrover.com
**KELLER GROVER LLP**
1965 Market Street
San Francisco, California 94103
Telephone: (415) 543-1305
Facsimile: (415) 543-7861

Timothy D. Cohelan, Esq. (SBN 60827)
tcohelan@ckslaw.com
Isam C. Khoury, Esq. (SBN 58759)
ikhoury@ckslaw.com
**COHELAN KHOURY & SINGER**
605 C Street, Suite 200
San Diego, California 92101
Telephone: (619) 595-3001
Facsimile: (619) 595-3000

SCOT BERNSTEIN (SBN 94915)
swampadero@sbernsteinlaw.com
**LAW OFFICES OF SCOT D. ERNSTEIN, A PROFESSIONAL CORPORATION**
101 Parkshore Drive, Suite 100
Folsom, California 95630
Telephone: (916) 447-0100
Facsimile: (916) 933-5533

Patrick N. Keegan, Esq. (SBN 167698)
pkeegan@keeganbaker.com
**KEEGAN & BAKER, LLP**
2292 Faraday Avenue, Suite 100
Carlsbad, California 92008
Telephone: (760) 929-9303
Facsimile: (760) 929-9260

*Attorneys for Plaintiffs*
Ryan Wu and Saber Khamooshi

*Attorneys for Plaintiff*
John Deddeh

**UNITED STATES DISTRICT COURT**

**NORTHERN DISTRICT OF CALIFORNIA**

IN RE: GANNETT CO. INTERNET TRACKING LITIGATION.

Case No: 3:24-cv-05150-MMC

**FIRST CONSOLIDATED CLASS ACTION COMPLAINT FOR DAMAGES AND INJUNCTIVE RELIEF**

**DEMAND FOR JURY TRIAL**

Action Filed: June 26, 2024
FAC Filed: July 23, 2024
Removed: August 14, 2024
SAC Filed: October 8, 2024
Consolidated: March 5, 2025

KELLER GROVER LLP
1965 Market Street, San Francisco, CA 94103
Tel. 415.543.1305 | Fax 415.543.7861

KELLER GROVER LLP
1965 Market Street, San Francisco, CA 94103
Tel. 415.543.1305 | Fax 415.543.7861

**FIRST CONSOLIDATED CLASS ACTION COMPLAINT**

Plaintiffs Ryan Wu, Saber Khamooshi, and John Deddeh, on behalf of themselves and a class of similarly situated individuals as defined below, and based on personal knowledge where applicable, information and belief, and investigation by counsel, allege the following against Defendant Gannett Co., Inc.

## INTRODUCTION

1. This class action lawsuit arises out of Defendant's policy and practice during the proposed class period of embedding and using various trackers on Defendant's USA Today website, www.usatoday.com, to (1) install and store third-party tracker cookies on California website users' browsers and (2) surreptitiously share and allow those third-party trackers to collect California website users' browser and device/operating system data as well as personally identifying and addressing information, such as IP addresses[1]. Defendant did all of that without users' knowledge, authorization, or consent.

2. Defendant Gannett Co., Inc. ("Defendant" or "Gannett") is an American mass media company that owns and publishes various brands that deliver journalism, compelling content, events, experiences, and digital marketing business solutions. Gannett's portfolio includes hundreds of brands and local media outlets across the United States and the United Kingdom, including USA Today, The Arizona Republic, Golfweek, Newsquest Media Group, and many others. Gannett also owns and operates a number of daily newspapers in California that provide local news stories, content, and relevant local advertising. Those include The Desert Sun, The Salinas Californian, Visalia Time-Delta, Record Searchlight, Ventura County Star, Victorville Daily Press, Tulare Advance Register, and The Stockton Record.

3. Founded in 1980 and launched in 1982, USA Today is a newspaper and news broadcasting company that operates from Gannett's corporate headquarters in New York. USA

[1] IP addresses have been classified by the United States Department of Health and Human Services ("HHS") as personally identifying information. *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates*, U.S. Department of Health and Human Services (Dec. 1, 2022), https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html (last visited May 8, 2025).

Today covers breaking news, politics, sports, entertainment, money, wellness and more. Its newspaper is printed at 37 sites across the United States, including at one production facility in California, and at five additional sites internationally. Defendant also owns and operates the www.usatoday.com website (the "USA Today website"), which provides breaking news and coverage of U.S. and national news.

4. Plaintiffs and Class members who visit the USA Today website expect that their personally identifying information, including their IP addresses, will remain private and confined to their use of the USA Today website. Plaintiffs and Class members have a reasonable expectation that their accessing of and interactions with the USA Today website will not be sold for advertising purposes or shared with any third parties, let alone to *undisclosed* third-party trackers.

5. Unbeknownst to individuals entering and viewing the USA Today website, third-party trackers are embedded into Defendant's website. Through that embedded tracking technology, while Plaintiffs and Class members were and are accessing and interacting with the USA Today website, Defendant was and is (1) installing and storing third-party tracker cookies on users' browsers and (2) disclosing and sharing USA Today website users' browser and device/operating system data, IP addresses, and other identifying information to and with those third-party trackers. All of this happens the moment users enter the USA Today website and without any further action required by or requested of the users. And it happened without any meaningful notice.

6. Plaintiffs are informed and believe and, on that ground, allege that Defendant caused the collection of and surreptitiously shared identifying data, including addressing information such as IP addresses, with the third-party trackers for advertising and analytics-related purposes. Defendant did so without obtaining USA Today website users' authorization or consent and without a court order.

7. Defendant's unauthorized (1) installation of third-party tracker cookies on California users' web browsers and (2) disclosure to and collection by third parties of Plaintiffs' and Class members' personally identifying and addressing information, all without consent or

KELLER GROVER LLP
1965 Market Street, San Francisco, CA 94103
Tel. 415.543.1305 | Fax 415.543.7861

adequate notification to Plaintiffs and Class members, were invasions of Plaintiffs' and Class members' privacy. Defendant's actions also violate multiple laws, including the California Computer Data Access and Fraud Act, Cal. Penal Code § 502 ("CDAFA"); the California Invasion of Privacy Act, Cal. Penal Code §§ 630, *et seq.* ("CIPA"); the right to privacy under Article 1, § 1, of the California Constitution, which includes privacy as one of six fundamental rights of all Californians; and the Unfair Competition Law, California Business & Professions Code §§ 17200, *et seq.* ("UCL").

## PARTIES

### A. Plaintiffs Ryan Wu, Saber Khamooshi, and John Deddeh

8. Plaintiffs are natural persons and residents of California.

9. While physically present in California, Plaintiff Wu regularly has visited and still visits the USA Today website to browse news headlines and read articles. He visited the USA Today website as recently as May 2024. Plaintiff Wu used and continues to use an internet browser on his computer and on his cellular phone to access Defendant's website.

10. While physically present in California, Plaintiff Khamooshi regularly has visited and still visits the USA Today website to browse news headlines and read articles. He visited the USA Today website as recently as June 2024. Plaintiff Khamooshi used and continues to use an internet browser on his computer and on his cellular phone to access Defendant's website.

11. While physically present in California, Plaintiff Deddeh used an internet browser on his computer and on his cellular telephone to access the USA Today website during the past three years to browse news headlines and read articles. Plaintiff Deddeh used and continues to use an internet browser on his computer and on his cellular phone to access Defendant's website.

12. At no time when Plaintiffs entered the USA Today website and viewed its content during the proposed class period did Plaintiffs authorize Defendant to install or consent to Defendant installing third-party tracker cookies on their internet browsers or computers.

13. Plaintiffs also did not consent to Defendant sharing and selling their browser and device/operating system data, IP addresses and other personally identifying information with or to third-party trackers. Further, because Defendant did not provide notice or request permission,

KELLER GROVER LLP
1965 Market Street, San Francisco, CA 94103
Tel. 415.543.1305 | Fax 415.543.7861

Plaintiffs were unaware of and had no meaningful opportunity to opt out of or object to that unauthorized disclosure of their data.

**B. Defendant Gannett Co., Inc. and the USA Today Website**

14. Defendant Gannett Co., Inc. is a corporation organized under the laws of the State of Delaware with its headquarters and principal place of business in New York, New York.

15. Defendant systematically and continuously does business in California and with California residents. In order to do so, Defendant is registered with the California Secretary of State and has an agent for service of process in California.

16. In parallel with its national publications, Defendant also owns and operates local brands, ***including eight daily publications in California***:

(a) The Desert Sun in Palm Springs, California;

(b) The Salinas Californian in Salinas, California;

(c) Visalia Times-Delta in Visalia, California;

(d) Redding Record Searchlight in Redding, California;

(e) Ventura County Star in Camarillo, California;

(f) The Stockton Record in Stockton, California;

(g) Victorville Daily Press in Victorville, California; and

(h) Tulare Advance Register in Tulare, California.

17. The website for each of these California daily publications states that the local brand is a part of the USA TODAY Network and is owned and operated by Gannett Co., Inc.

18. Each of the California daily publications covers local content specific to its area under the headings "Local News" and "More Local News." The website for each also publishes national content that is shared between and among Defendant's numerous brands. In addition to the local news, the website for each California publication has a "Marketplace" for local advertisements, classified advertisements, and public notices.

19. Defendant's California-centered websites also state proudly that they support local businesses in a number of cities, including four large cities in California: San Francisco (156 businesses); Los Angeles (151 businesses); Palm Desert (150 businesses); and Redding (139

KELLER GROVER LLP
1965 Market Street, San Francisco, CA 94103
Tel. 415.543.1305 | Fax 415.543.7861

businesses). When a user chooses a California city under the "Support Local Businesses" link, the website displays an alphabetical list of local businesses supported, their contact information, and a link that redirects a user to the website of the local California business.

20. To carry out its numerous business activities inside of California, Defendant employs individuals within and around California. At the beginning of May 2025, under the "Careers" tab on the Gannett website, there were at least 11 job postings listed in six different cities/counties in California to add to Gannett's California workforce. Those locations include Orange County, Woodland Hills/Los Angeles, San Diego County, Victorville, Camarillo, and Stockton.[2]

21. Similarly, Defendant maintains various offices throughout California. Those include a corporate office in Los Angeles with departments for Sales, Accounting, Engineering, Marketing and Business Development, among others. Gannett also has a retail office in San Francisco, California, to handle sales, marketing and business development. A number of the California daily publications also have offices in cities such as Palm Desert, Palm Springs, Redding, and Salinas.

22. As part of its mass-media holdings, Defendant currently owns and operates USA Today and its interactive website, www.usatoday.com. That website publishes breaking news and articles regarding politics, sports, entertainment, money-related matters, wellness, and more from across the United States and around the world.

23. Although Defendant's USA Today website provides a chat function and a toll-free number for Californians to "[g]et in touch with [Gannett] about stories happening in [their] community," the website fails to put visitors on notice of Defendant's use of website tracking technology, including its use of third-party trackers. Upon information and belief, Plaintiffs allege that third-party trackers allow and enable companies like and including Defendant to sell advertising space on their websites by using the tracking technology to receive, store and, analyze information collected surreptitiously from website visitors.

---

[2] Search Jobs, Gannett, https://www.gannett.com/search-jobs/ (last visited May 8, 2025).

KELLER GROVER LLP
1965 Market Street, San Francisco, CA 94103
Tel. 415.543.1305 | Fax 415.543.7861

KELLER GROVER LLP
1965 Market Street, San Francisco, CA 94103
Tel. 415.543.1305 | Fax 415.543.7861

24. The USA Today website also failed and fails to disclose the selling and sharing of browser and device/operating system data and personally identifying information, including IP addresses and other addressing information, to and with unauthorized third party-trackers for advertising and other purposes.

**JURISDICTION AND VENUE**

25. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act ("CAFA"), 28 U.S.C. § 1332(d). Specifically, this action satisfies all requirements for federal jurisdiction under CAFA in that the allegations in this Complaint identify a putative class of more than 100 members, establish the minimum diversity of citizenship required under CAFA, and place in controversy more than $5 million in the aggregate for the entire class, exclusive of interest and costs. 28 U.S.C. § 1332(d) and (d)(5) and § 1453(b).

26. This Court has personal jurisdiction over the parties because Defendant has sufficient minimum contacts with this State in that it operates its numerous brands and businesses within and markets its services and products throughout the State, including California-specific news offerings and directing targeted advertising to California residents. As described in Paragraphs 15 through 21, Defendant's activities in California are substantial, continuous, and systematic. In addition to its production facility located in California, Defendant owns and operates eight California daily newspapers, each focusing on local news and content, promoting local California businesses, and serving local regional advertisements. To conduct its numerous business activities within California and support its local brands, Defendant employs California residents and maintains offices in various cities throughout California. In describing its local brands, Defendant's website states: ***"For the community, by the community. Our local brands are engrained in the places we call home."***

27. In addition to its media holdings in California, Defendant also owns a number of subsidiaries that are either incorporated in or organized under the laws of the State of California. These include Defendant's digital marketing services companies under the brand LocaliQ. LocaliQ is headquartered in Woodland Hills, California and has sales and other offices in Irvine, Los Angeles, and San Francisco, California, as well as in Texas. Defendant's other California

KELLER GROVER LLP
1965 Market Street, San Francisco, CA 94103
Tel. 415.543.1305 | Fax 415.543.7861

subsidiaries, which are organized under California law, include Salinas Newspapers LLC, SureWest Directories, The Desert Sun Publishing Co., The Sun Company of San Bernardino, California, and Visalia Newspapers LLC.

28. Further, a substantial part of the events and conduct giving rise to Plaintiffs' claims occurred in the State of California. Those events and that conduct included Plaintiffs' accessing of and interactions with the USA Today website, Defendant's unauthorized installation of third-party tracker cookies on California users' web browsers, and the disclosure and surreptitious sharing of Plaintiffs' and Class members' browser and device/operating system data and personally identifying and addressing information with the third-party trackers, all without users' knowledge, authorization or consent. By causing a digital transmission to enter California, Defendant deliberately reached out beyond its home state, in a manner that was neither random, isolated, nor fortuitous, by knowingly installing tracking software on unsuspecting Californians' browsers so that it could later sell the data it obtained. The "brunt of the harm" of these privacy violations was suffered in the State of California, and those violations arose out of Plaintiffs' contact with Defendant from and within the State of California.

29. Moreover, Defendant's conduct was directed at California. Defendant operated its interactive USA Today website to sell its products, marketed that website directly to Californians, installed trackers on their devices in California, and profited from its intentional exploitation of that market and location-specific advertising. In essence, Defendant knows about its California consumer base, conducts its regular business in California, has contact and interacts with California residents, installs software onto their browsers in California, and continues to track their activities. Thus, by targeting its wrongful conduct at website consumers, some of whom it knew, at least constructively, to be residents of California, Defendant expressly aimed its conduct at California.

30. Venue is proper in this Court because Defendant removed the action from San Francisco County Superior Court. Venue was proper in that court under Code of Civil Procedure §§ 395 and 395.5 and case law interpreting those sections, which provide that if a foreign business entity fails to designate with the office of the California Secretary of State a principal place of

KELLER GROVER LLP
1965 Market Street, San Francisco, CA 94103
Tel. 415.543.1305 | Fax 415.543.7861

business in California, it is subject to being sued in any county that a plaintiff desires. On information and belief, Defendant Gannett Co., Inc. is a foreign business entity and, as of the date on which the Complaint in this action originally was filed, had failed to designate with the Office of the Secretary of State, a principal place of business in California.

**STANDING**

31. Article III standing is met when a plaintiff "(1) suffered an injury in fact, (2) that is fairly traceable to the challenged conduct of the defendant, and (3) that is likely to be redressed by a favorable judicial decision." *Spokeo, Inc. v. Robins*, 578 U.S. 337, 338 (2016).

32. Plaintiffs meet the "injury in fact" requirement because the invasion of their privacy is a "concrete and particularized" injury. *See TransUnion LLC v. Ramirez*, 141 S. Ct. 2190, 2204 (2021), stating that "Various intangible harms can also be concrete [including] . . . disclosure of private information"; and *In re Facebook Inc. Internet Tracking Litig.*, 956 F.3d 589, 596 (9th Cir. 2020), holding that Facebook's tracking of browsing histories that were sold to advertisers was an "invasion of [a] legally protected interest that is concrete and particularized."

33. Plaintiffs allege that they were personally injured when Defendant impermissibly obtained, disclosed, and shared Plaintiffs' personal information with third parties without consent or authorization. It is black-letter law that such allegations are sufficient to confer Article III standing. *See, e.g.*, *Mastel v. Miniclip SA*, 2021 WL 2983198, at *6 (E.D. Cal. July 15, 2021), stating that collection of "personal information without the plaintiff's consent involved a sufficiently 'concrete' injury"; *In re Facebook, Inc., Consumer Privacy User Profile Litig.*, 402 F.Supp.3d 767, 784 (N.D. Cal. 2019), holding that dissemination to third parties of plaintiffs' personal information is "sufficient to confer [Article III] standing."

34. Separate from an invasion-of-privacy harm, Plaintiffs also allege economic harm sufficient for Article III standing by alleging that user data carries financial value. For example, Google's Online Insight Study will pay users "up to $130 per year" to record participants' data

KELLER GROVER LLP
1965 Market Street, San Francisco, CA 94103
Tel. 415.543.1305 | Fax 415.543.7861

"browsing the web."[3] Similarly, Nielson operates a Computer & Mobile Panel where users can receive up "[u]p to $60" in benefits to sign up "computers, smartphone, and tablets" for tracking.[4] Indeed, in a recent SEC filing Defendant states its intention to "fully monetize the numerous visitors to our digital platforms" through "digital advertising," but specifically warns investors that "enhanced data privacy, could materially and adversely impact our advertising revenues and business results."[5]

35. The Ninth Circuit has found such allegations to be sufficient to establish Article III standing under a theory of economic harm. *See Facebook Tracking*, 956 F.3d at 600 ("[Plaintiffs] point to the existence of a study that values users' browsing histories at $52 per year, as well as research panels that pay participants for access to their browsing histories."). Further, "[u]nder California law, this stake in unjustly-earned profits exists regardless of whether an individual planned to sell his or her data or whether the individual's data is made less valuable." *Facebook Tracking*, 956 F.3d at 600.

36. Plaintiffs' injuries are "fairly traceable" to Defendant's challenged conduct[6] because Defendant acquired and shared Plaintiffs' private information using third-party trackers that are embedded into the USA Today website. Plaintiffs' injuries therefore occurred the moment their information was acquired improperly by Defendant.

37. Plaintiffs also meet the redressability element because courts consistently have recognized that violations of privacy rights can be redressed by an award of damages or injunctive relief. *See Facebook Privacy*, 402 F.Supp.3d at 784, stating that "[T]he Ninth Circuit has repeatedly explained that intangible privacy injuries can be redressed in the federal courts." *See*

---

[3] Online Insights Study, Google, https://onlineinsightsstudy.google/signup (last visited May 7, 2025).

[4] Computer & Mobile Panel, Nielson, https://computermobilepanel.nielsen.com/ui/US/en/sdp/landing (last visited May 7, 2025).

[5] Gannet Co., Inc., Annual Report (Form 10-K) for Fiscal Year 2024, at 5, 18 (Feb. 20, 2025), *available at https://s202.q4cdn.com/162862548/files/doc_financials/2024/q4/GCI-2024-12-31-10K_2025-02-20FINAL.pdf* (last visited May 7, 2025).

[6] *Spokeo*, 578 U.S. at 338.

KELLER GROVER LLP
1965 Market Street, San Francisco, CA 94103
Tel. 415.543.1305 | Fax 415.543.7861

*also Jewel v. Nat'l Sec. Agency*, 673 F.3d 902, 912 (9th Cir. 2011) (similar). Additionally, the injunctive relief that Plaintiffs seek includes terminating all downstream distributions of that illegally collected personal data. That is a remedy that would redress future harms suffered by Plaintiffs and the Class and would have the potential to prevent those future harms.

## FACTUAL ALLEGATIONS COMMON TO THE CLASS

### A. Website Tracking Technology

38. "Third-party tracking refers to the practice by which a tracker, other than the website directly visited by the user, traces or assists in tracking the user's visit to the site."[7] Trackers use cookies, scripts, or pixels inserted by publishers or advertisers to collect information about internet users as those users are browsing the web, including capturing IP addresses and other device information such as device type, browser type, and unique and persistent identifiers ("device fingerprints"). The trackers also cause additional data points to be sent from users' browsers to the third parties. Those additional data points are intended to identify users uniquely across sessions and devices and to track those users pervasively across the internet.

39. Tracker profiling is the process of linking data from different websites to build user profiles based on the users' browsing history, to place those users into categories or groups, and to sell that data to third parties so that those third parties can use it for targeted advertising. "If the same third-party tracker is present on many sites, it can build a more complete profile of the user over time."[8]

40. A broad range of online technologies track and monitor internet-based interactions and communications. Four identifier tools that commonly are used are (i) website cookies, (ii) tracking pixels, (iii) digital fingerprinting, and (iv) software development kits.

41. A website cookie is a small text file that a website server creates and transmits to a web browser (*e.g.*, Google Chrome or Safari). That web browser then installs and stores the file

---

[7] *Third-party Tracking*, PIWIK, https://piwik.pro/glossary/third-party-tracking/ (last visited May 7, 2025).

[8] *Id.*

in a particular directory on an individual's computer, phone or other device.[9] When a website user attempts to access a webpage, the user's browser transmits a communication to the website's server requesting that the server display the website's content for the browser to load. While providing the requested content to the user, the website's server also provides the cookies that it would like the user's browser to install and retain.

42. Website cookies contain information that identifies the domain name of the webserver that wrote the cookie (*e.g.*, www.hulu.com or www.facebook.com). Cookies also have information about the user's interaction with a website, such as how the website should be displayed, how many times a user has visited the website, how long a user spends on a webpage, information about what pages the user visited, and authentication information. In addition to a unique identifier and a site name, website cookies also can include personally identifiable information such as a user's name, address, email address or telephone number if that information was provided to a website.

43. A **first-party cookie** is implemented by the website that the user accesses. The website uses first-party cookies for authentication, monitoring user sessions, and collecting analytical data.

44. In contrast, a **third-party cookie**, also called an "advertising cookie" or a "tracker cookie," is a cookie that belongs to a domain other than the one being displayed to the user in his or her browser. A third-party cookie typically is used for cross-site tracking, retargeting and ad-serving. The key differences between the first-party and third-party cookies are who sets them (*i.e.*, a website display host or a third party), whether and how they can be blocked by a web browser, and the availability of the cookie. A third-party advertising or tracker cookie is available and accessible on *any* website that loads the third-party server's code, not just on the host website that the user is trying to access.

45. A pixel, also known as a "tracking pixel," "web bug," "clear GIF" or "web beacon,"

[9] *See* Sara J. Nguyen, *What Are Internet Cookies and How Are They Used?*, All About Cookies (July 28, 2023), https://allaboutcookies.org/what-is-a-cookie (last visited May 7, 2025).

KELLER GROVER LLP
1965 Market Street, San Francisco, CA 94103
Tel. 415.543.1305 | Fax 415.543.7861

is similar to a website cookie. It is a small, almost invisible image (pixel) embedded in a website or an email to track a user's activities. That tracked data often includes information regarding the user's operating system, the type of website or email used, the time when the website was accessed, the user's IP address, and whether there are cookies that previously have been set by the server hosting the pixel image.[10]

46. "Digital fingerprinting" refers to device fingerprinting and browser fingerprinting, both of which send information to the website server to help ensure that a website is displaying content correctly and operating appropriately. ***Although a browser or device does not usually transmit personal information about a user, most fingerprinting is performed via a third-party tracker, which can track an individual across multiple sites and form a profile of the user.***[11]

47. A software development kit ("SDK") is a set of computer programs and similar tools that developers and engineers can leverage to build applications for specific platforms. The SDK often includes, among other tools, libraries, application programming interfaces, instructions, guides, directions, and tutorials.[12] SDKs also may have embedded code that allows them to intercept personal data and other information from application users surreptitiously, including geolocation data, usernames and communications derived from other SDK applications installed on a user's device, and a user's activities within an application after installation.

48. All of the information and data captured and collected by third-party trackers, regardless of the tool used, is capable of being sold and used for marketing and advertising purposes.

**B. Internet Protocol Addresses ("IP Addresses")**

49. One important piece of identifying information collected by third-party trackers is

---

[10] *See* Patti Croft & Catherine McNally, *What Is a Web Beacon and Why Should You Care?*, All About Cookies (Feb. 19, 2025), https://allaboutcookies.org/what-is-a-web-beacon (last visited May 7, 2025).

[11] See Anokhy Desai, *The Half-Baked Future of Cookies and Other Tracking Technologies*, IAPP (July 2023), https://iapp.org/resources/article/future-of-cookies-tracking-technologies/ (last visited May 7, 2025).

[12] *See What Is an SDK? Software Development Kits Explained*, Okta, Inc. (Apr. 2, 2025), https://www.okta.com/identity-101/what-is-an-sdk/ (last visited May 7, 2025).

KELLER GROVER LLP
1965 Market Street, San Francisco, CA 94103
Tel. 415.543.1305 | Fax 415.543.7861

a website user's IP address. An IP address is a unique identifier for a device connected to the internet, and is a numerical code written as four sets of numbers separated by periods (e.g., 123.145.167.189). The first two sets of numbers reflect what network the device is on; the second two sets of numbers identify the specific device.

50. An IP address is essential for identifying a specific device on the internet or within a local network. It facilitates communication between devices, and allows a communication signal to be routed from one identified device to another identified device.

51. A **private IP address** is used within an internal network and is assigned within a specific range of numbers designated exclusively to be used for private IP addresses. A private IP address is not routable on the internet, and thus can be used simultaneously, without conflict, in different private or local networks because they are isolated from the global internet. Non-unique private IP addresses conserve the finite number of combinations that make an IP address and facilitate local network communications.

52. In contrast, **public IP addresses** are required for devices that need direct internet access and are assigned by an Internet Service Provider ("ISP"). Because a public IP address is accessible from anywhere on the internet, it is unique to a device globally. Although the term "public" is used, a public IP address is not freely accessible. If a device is not actively sending out data, the public IP address remains private and is not broadcast to the wider internet. Unique public IP addresses facilitate global communications.

53. Significantly, public IP addresses contain geographical location information from which the state, city, and zip code of a specific device can be determined. Various services, such as iplocation.io, use databases to map IP addresses to physical locations in geographic areas, and often can provide information about the country, city, and approximate latitude and longitude coordinates of a specific device. In some instances, even the ISP associated with the public IP address can be determined. This geolocation capability is leveraged and used extensively in online advertising and user identification services.

54. Given the information that it can and does reveal, an IP address is considered

KELLER GROVER LLP
1965 Market Street, San Francisco, CA 94103
Tel. 415.543.1305 | Fax 415.543.7861

personally identifiable information and is subject to HIPAA protection.[13] Under California law, an IP address also is considered an identifier and constitutes a consumer's protected personal information.[14] Further, under Europe's General Data Protection Regulation, IP addresses are considered "personal data, as they can potentially be used to identify an individual."[15]

55. While a private IP address does not disclose a user's geolocation information, a public IP address does divulge such personal information. A public IP address reveals the approximate location of the user who is connecting to the internet and the router that is directing those communications. That is often the user's house or workplace.

56. Knowing a website user's public IP address, and therefore the user's geographic location, provides "a level of specificity previously unfound in marketing."[16] A public IP address allows advertisers to target customers by countries, cities, neighborhoods, and postal codes.[17] Even more specifically, it allows advertisers to target specific households, businesses, and even individuals with ads that are relevant to their interests by matching physical addresses to IP addresses.[18]

57. Indeed, IP targeting is one of the most successful marketing techniques that companies can employ to spread the word about a product or service because companies are

---

[13] *See* 45 C.F.R. § 164.514(b)(2)(i)(O).

[14] *See* Cal. Civ. Code § 1798.140(v)(1)(A).

[15] *Is an IP Address Personal Data?*, Convesio, https://convesio.com/knowledgebase/article/is-an-ip-address-personal-data/ (last visited May 8, 2025); *see also What is Personal Data*, European Commission, https://commission.europa.eu/law/law-topic/data-protection/reform/what-personal-data_en/ (last visited May 8, 2025).

[16] *IP Targeting: Understanding This Essential Marketing Tool*, AccuData, https://www.accudata.com/blog/ip-targeting/, *archived at* https://web.archive.org/web/20240326190403/https://www.accudata.com/blog/ip-targeting/ (last visited May 8, 2024).

[17] *Location-based Targeting That Puts You in Control*, Choozle, https://choozle.com/geotargeting-strategies/ (last visited May 8, 2025).

[18] Herbert Williams, *The Benefits of IP Address Targeting for Local Businesses*, LinkedIn (Nov. 29, 2023), https://www.linkedin.com/pulse/benefits-ip-address-targeting-local-businesses-herbert-williams-z7bhf/ (last visited May 8, 2025).

KELLER GROVER LLP
1965 Market Street, San Francisco, CA 94103
Tel. 415.543.1305 | Fax 415.543.7861

incentivized and can use a public IP address to identify individuals personally.[19] By targeting specific households or businesses, a company can avoid wasting money on ads that are unlikely to be seen by their target audience and can reach their target audience with greater precision.[20] Additionally, by analyzing data on which households or businesses are responding to their ads, IP address targeting can help businesses improve their overall marketing strategies and refine their marketing efforts.[21]

58. "IP targeting capabilities are highly precise, with an accuracy rate of over 95%. This means that advertisers can deliver highly targeted ads to specific households or businesses, rather than relying on more general demographic or behavioral data."[22]

59. Public IP addresses also are used for "geomarketing," which is "the practice of using location data to identify and serve marketing messages to a highly targeted audience."[23] The core principle of geomarketing is that "where you are is who you are." By identifying target audiences that work, live, or vacation in a specific location, geomarketing allows businesses (and their websites) to determine consumers' wants and needs based on location-related factors and to tailor their marketing to the products or services that appeal to those needs.[24]

60. As alleged below, Defendant installed and continues to install third-party tracker cookies on USA Today website users' browsers. Those trackers unlawfully have collected and continue to collect browser and device/operating system data as well as identifying and addressing information about Plaintiffs and Class members, including their IP addresses. They have done so

---

[19] Trey Titone, *The future of IP address as an advertising identifier*, Ad Tech Explained (May 16, 2022), https://adtechexplained.com/the-future-of-ip-address-as-an-advertising-identifier/ (last visited May 8, 2025).

[20] Herbert Williams, *The Benefits of IP Address Targeting for Local Businesses*, LinkedIn (Nov. 29, 2023), https://www.linkedin.com/pulse/benefits-ip-address-targeting-local-businesses-herbert-williams-z7bhf/ (last visited May 8, 2025).

[21] *Id.*

[22] *IP Targeting*, Savant DSP, https://www.savantdsp.com/ip-targeting/ (last visited May 5, 2025).

[23] *See, e.g., Geomarketing Strategies & Tips: The Essential Guide*, Deep Sync (Jan. 3, 2025), https://deepsync.com/geomarketing/ (last visited May 8, 2025).

[24] *Id.*

KELLER GROVER LLP
1965 Market Street, San Francisco, CA 94103
Tel. 415.543.1305 | Fax 415.543.7861

without a court order and without Plaintiffs' or Class members' consent.

**C. Defendant's Use of Third-Party Trackers on the USA Today Website**

61. Defendant has embedded and implemented several third-party trackers on the USA Today website, including but not limited to (i) Taboola Tracker, (ii) Amobee Tracker, and (iii) Adnxs Tracker (the "trackers"). By installing these trackers and their corresponding tracking cookies, Defendant can sell advertising space on the USA Today website. That enables Defendant to monetize its website further, maximize its revenue by disclosing/selling user information, and obtain and analyze users' data for its own profit.

62. When a website user first accesses and enters the USA Today website, the user's browser sends an HTTP[25] request to Defendant's server. The USA Today website server then sends an HTTP response with directions to load the webpage content. In addition to the webpage details, the USA Today website server also sends instructions, as programmed by Defendant, and causes the three trackers to be installed on the user's browser. The trackers, in turn, instruct the user's browser to send the third-party trackers the user's identifying and addressing information, including but not limited to the user's IP address and device fingerprints.

63. Each tracker installs and stores its own website cookie on the user's browser and uses that third-party tracker cookie to collect and share that user's browser and device data and addressing information, including IP addresses, every time the user visits and interacts with the USA Today website. ***Some of the data points sent from USA Today website users' browsers to the third parties are meant to identify users uniquely across sessions and devices, allowing for cross-site tracking and behavioral profiling of those individuals***.

64. The process described above takes place behind the scenes and in less than a second. Thus, the three tracker cookies appear and are implemented the instant the user enters the USA Today website. No further action, clicks, or consent from the user are required.

65. Further, each of the three trackers embedded on Defendant's website re-installs its

[25] HTTP stands for "HyperText Transfer Protocol." It is the computer communication protocol used for most communication on the world wide web.

KELLER GROVER LLP
1965 Market Street, San Francisco, CA 94103
Tel. 415.543.1305 | Fax 415.543.7861

KELLER GROVER LLP
1965 Market Street, San Francisco, CA 94103
Tel. 415.543.1305 | Fax 415.543.7861

tracker cookies every time a user visits the USA Today website. Thus, even if a user clears the cookies from the user's browser, it makes no difference: the next time that user visits the USA Today website, all three trackers re-install their tracker cookies, reset the tracking process, and resume transmission of the user's browser and device data, IP address, and other identifying information to the undisclosed third parties.

66. At no time before to the installation and use of the trackers on USA Today website users' browsers did Defendant procure users' consent for that conduct. Nor did Defendant obtain a court order to install or use any of the three trackers.

67. The **Taboola Tracker** is developed by software company Taboola Inc., which uses data analytics to correlate digital content with user preferences across its network of publisher websites. As a content recommendation platform, the Taboola Tracker is designed to collect user data to optimize content suggestions, enhancing both user experience and content monetization for publishers. Specifically, Taboola collects IP addresses to allow it to ascertain a user's location and to target that user with advertisements tailored to that specific location. According to its website, Taboola uses its "unique data about people's interests and information consumption to recommend the right content to the right person at the right time."[26] Taboola assists advertisers with targeting their campaigns by location, time, browser type, connection type, audience segments, and more.[27] Taboola allows advertisers to target based on "who is visiting or interacting with your site" and allows profiling of "people who have visited a certain section of your site."[28] Taboola even allows companies to upload information about existing customers using "Emails or Mobile IDs" and then target a campaign based on the additional information Taboola gathers.[29] Critically, Taboola

---

[26] *How Taboola Works*, Taboola Help Center, https://help.taboola.com/hc/en-us/articles/115006597307-How-Taboola-Works (last visited May 8, 2025).

[27] *Id.*

[28] Building and Targeting Advertiser Website ("My") Audience, https://help.taboola.com/hc/en-us/articles/360003504813-Building-and-Targeting-Advertiser-Website-My-Audiences (last visited May 8, 2025).

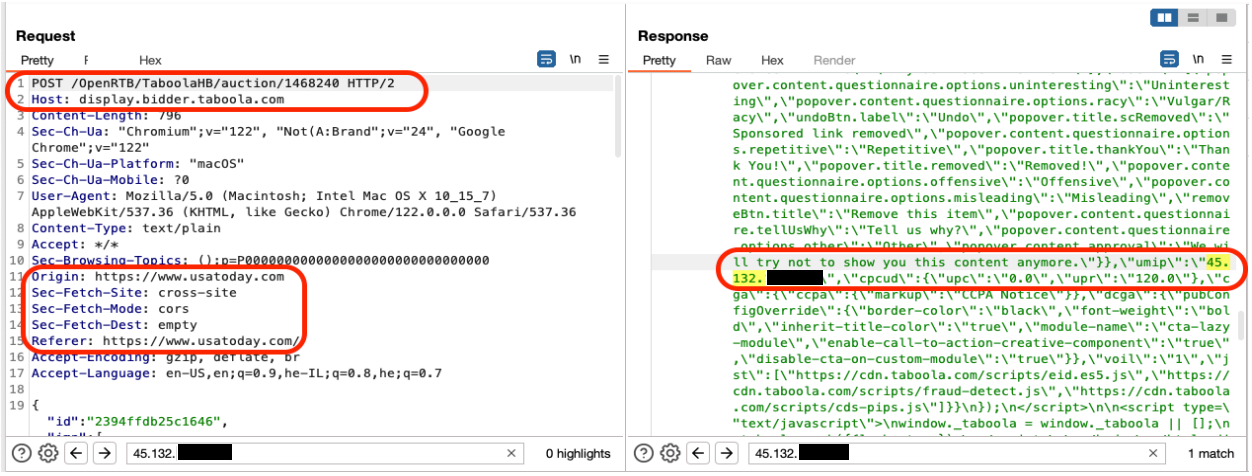
[29] Uploading and Targeting a Customer File, https://help.taboola.com/hc/en-us/articles/360021908874-Uploading-and-Targeting-a-Customer-File (last visited May 8, 2025).

KELLER GROVER LLP
1965 Market Street, San Francisco, CA 94103
Tel. 415.543.1305 | Fax 415.543.7861

"identifies users who've already visited your website or specific pages."[30]

68. When a user visits the USA Today website, the Taboola Tracker installs and stores its website cookie on the user's browser. This third-party tracker cookie is used to collect and share that user's browser and device data, IP address, and other identifying information with third-party Taboola Inc. That, in turn, enables Taboola to serve personalized, targeted advertisements and to optimize and maximize user engagement. ***Taboola receives a user's personal data, including IP address and device fingerprints, each and every time the user interacts with the USA Today website.*** *See* Figure 1, identifying Taboola, www.usatoday.com, and the user's IP address (45.132.xxx.xxx).

**Figure 1**:




69. The **Amobee Tracker** is developed by Amobee, a digital marketing technology company that delivers a broad spectrum of advertising solutions aimed at helping brands, agencies, and publishers navigate the digital landscape. With an ad-serving platform that integrates across various channels such as digital, social, mobile and video, Amobee delivers targeted advertising content to users based on their browsing habits and other collected data, *including their IP addresses*. Amobee utilizes HTTP requests and responses, along with cookies and IP addresses, to track and deliver personalized ads to users on host sites like USA Today. Amobee cites its

[30] Taboola Pixel Overview, https://help.taboola.com/hc/en-us/articles/360003469854-Taboola-Pixel-Overview (last visited May 8, 2025).

ability to "reach users at the person level."[31] Indeed, Amobee claims that it can "[a]chieve **true identity** marketing" that "allows marketers to **make real-time, user-level decisions**, resulting in tight controls that maximize unique reach and avoid overexposure."[32]

70. Defendant embeds Amobee's code on its USA Today website. That hidden code causes and enables Amobee to install and store the Amobee Tracker and its corresponding website cookie on users' browsers. Like the Taboola Tracker, the Amobee Tracker is installed the instant a user accesses the USA Today website, all without any notice to the user and without any request for permission from the user.

71. Specifically, when a user visits the USA Today website, an HTTP request is sent to Amobee's servers. The HTTP request includes the user's IP address and allows Amobee to identify the user's geographic location. Amobee's servers then leverage the information contained within the user's HTTP request to respond with targeted ads tailored to that user.

72. During the HTTP communication process, Amobee installs and stores its tracker cookies on the user's browser. Those cookies, which also store information regarding the user's browsing behavior, browser and device/operating data, and other identifying information, enable Amobee to recognize the user on subsequent visits to USA Today or to other websites within Amobee's advertising network. Amobee and Defendant thereby leverage the user's personal data and browsing preferences. *See* Figure 2, identifying Amobee, www.usatoday.com, and the user's IP address (45.132.xxx.xxx).[33]

[31] Plan Better with Amobee Advertising Solutions, Amobee, https://www.amobee.com/solutions/plan/ (last visited May 8, 2025).

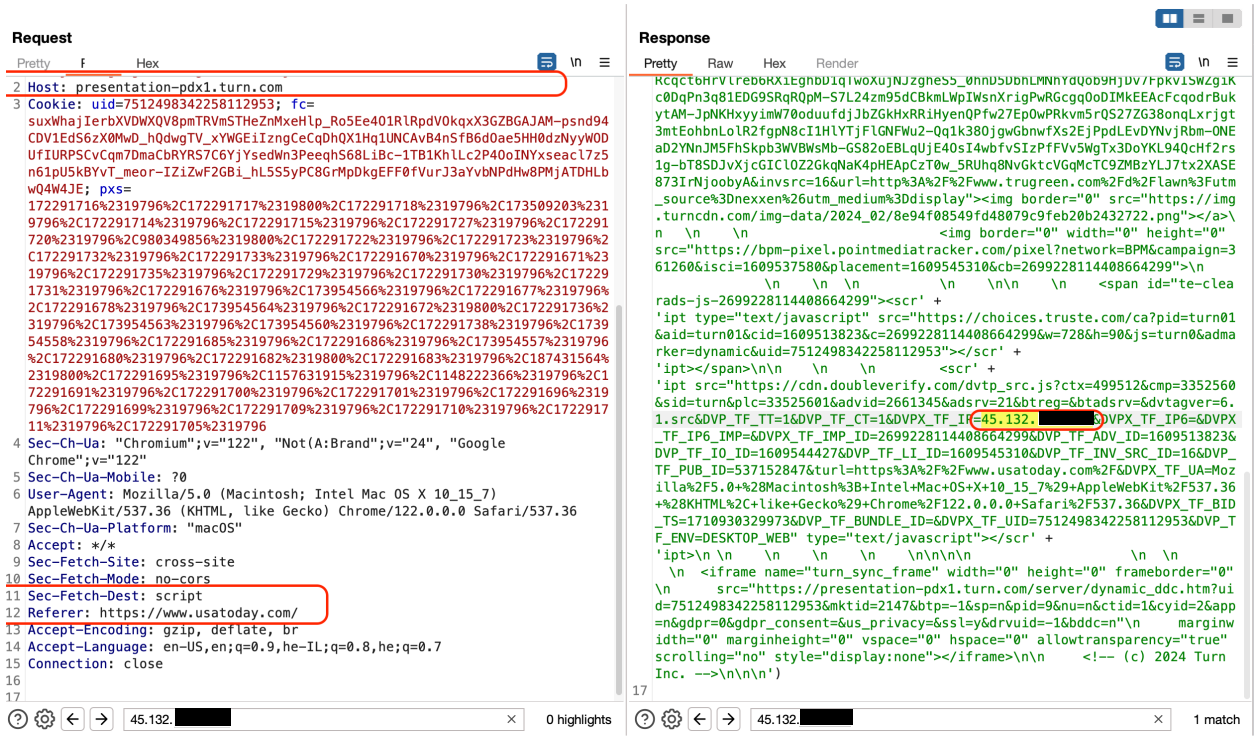
[32] *Id.* (emphasis added).

[33] The host name "presentation-pdx1.turn.com" signifies the presence of the Amobee tracker. Amobee is the name of the advertising platform, but its tracking cookies use the "turn.com" domain. *See* https://www.netify.ai/resources/domains/turn.com. ("The *.turn.com domain is associated with Amobee.") (last visited May 8, 2025).

KELLER GROVER LLP
1965 Market Street, San Francisco, CA 94103
Tel. 415.543.1305 | Fax 415.543.7861

KELLER GROVER LLP
1965 Market Street, San Francisco, CA 94103
Tel. 415.543.1305 | Fax 415.543.7861

**Figure 2**:



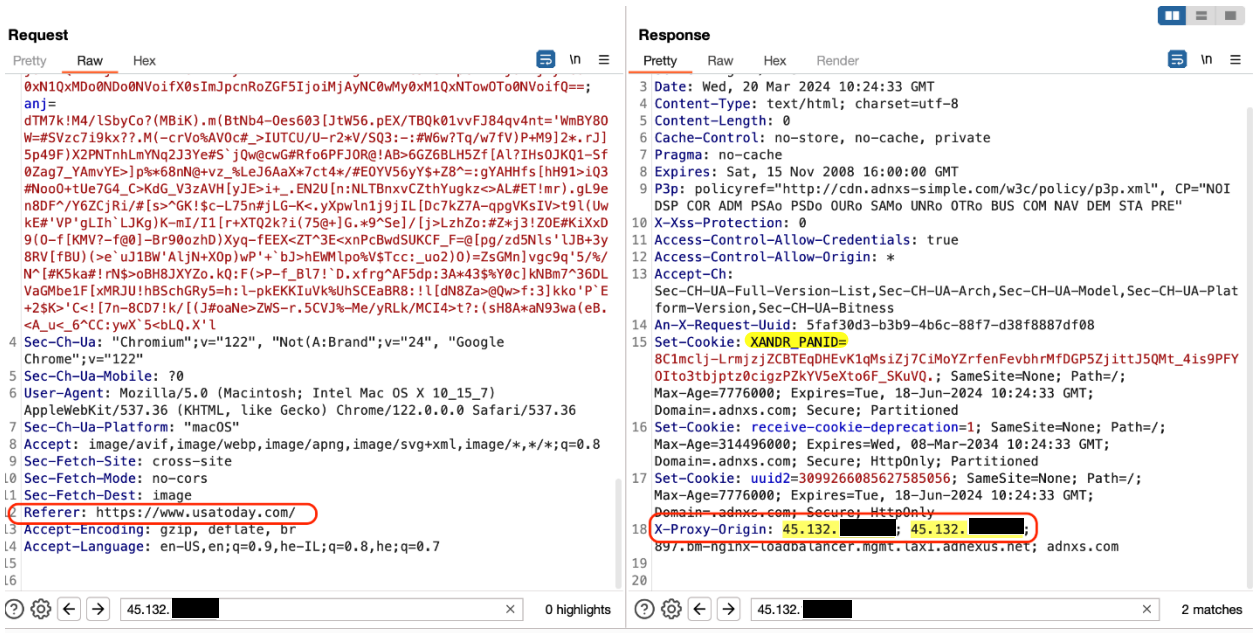

73. Even if the Amobee Tracker cookies are cleared from the user's browser, the Amobee Tracker is re-installed automatically and instantly on subsequent visits to USA Today. The tracking cycle restarts, ensuring that Amobee consistently receives the user's browser and device/operating system data, IP address, and browsing preferences with every website interaction. This mechanism facilitates a cycle of ad targeting and tracking and increases the relevancy and effectiveness of ads presented by Amobee to users across the web.

74. The third tracker embedded in Defendant's USA Today website is developed by software company Xandr, which Microsoft acquired in 2021. Xandr operates as an advanced advertising company that claims to provide a comprehensive platform for buying and selling consumer-centric digital advertising. The platform, which includes programmatic advertising, data analytics, and cross-screen media solutions, aims to improve the efficiency and effectiveness of advertising across various channels by leveraging data and technology.

75. Like other third-party trackers, Xandr allows companies like Defendant to sell advertising space on their websites by using the Adnxs Tracker to receive, store, and analyze information collected from website visitors. The **Adnxs Tracker** is installed and stored on the

user's browser the instant the user enters the USA Today website. The third-party tracker cookie then sends the user's IP address and device fingerprints to Xandr each and every time the user interacts with the USA Today website. *See* Figure 3, identifying Xandr, www.usatoday.com, and the user's IP address (45.132.xxx.xxx).

**Figure 3**:




76. Each of the three trackers embedded on Defendant's USA Today website (1) installs a third-party tracker cookie on users' browsers and (2) captures, collects, and shares with undisclosed third parties USA Today website users' personally identifying and addressing information, including the users' IP addresses and device fingerprints, ***all without the users' knowledge or consent***.

77. As alleged above, the trackers are designed to analyze USA Today website data, conduct hyper-targeted advertisements, and unjustly enrich and boost Defendant's revenue, all through the surreptitious collection and use of USA Today website users' public IP addresses, device fingerprints, and other information collected and set by the third-party trackers.

78. Notably, upon information and belief, the trackers collect IP addresses that can be used to ascertain a user's exact location, potentially with precise latitude-longitude coordinates and a zip code. As discussed above, Defendant and third parties can use that information to analyze

KELLER GROVER LLP
1965 Market Street, San Francisco, CA 94103
Tel. 415.543.1305 | Fax 415.543.7861

KELLER GROVER LLP
1965 Market Street, San Francisco, CA 94103
Tel. 415.543.1305 | Fax 415.543.7861

the USA Today website data and conduct targeted advertising based on a user's location.

79. Upon further information and belief, when a user entered or enters the USA Today website, all three trackers were and are used for real-time bidding ("RTB"). RTB is an online advertising auction that uses sensitive personal information to facilitate the process to determine which digital ad will be displayed to a user on a given website or application. Defendant's USA Today website uses the third-party trackers to "host" the bidding on Defendant's behalf, which happens almost instantly upon the visitor entering the website. The RTB system was designed to allow Defendant to sell targeted advertising and to maximize its revenue gained from selling ad space on the USA Today website.

80. During the RTB process, trackers will send user data to an advertising exchange, a platform that allows advertisers and publishers to exchange data, set prices, and ultimately serve an ad. The user data, often referred to as "bidstream data," includes information such as device identifiers, IP address, zip/postal code, GPS location, browsing history, location data, and more. After receiving the bidstream data, an advertising exchange will broadcast the data to several demand side platforms (DSPs), which then will examine the data to determine whether to make a bid on behalf of their advertising client. Ultimately, the winner of the bid will have its advertisement displayed to the user.[34]

81. Because most RTB auctions are held on the server/exchange side, instead of the client/browser side, the user sees only the winner of the auction and would not be aware of the advertisers that bid and lost. Nonetheless, even the losing advertisers benefit because they also receive and collect the user data that was broadcast during the RTB auction process. That surreptitiously exchanged information can be added to existing dossiers that advertisers have regarding users[35], further diminishing the ability of users to control their personal information.

82. As the Federal Trade Commission ("FTC") has noted, "[t]he use of real-time

---

[34] See *Real-Time Bidding*, Appsflyer, https://www.appsflyer.com/glossary/real-time-bidding/ (last visited May 5, 2025).

[35] *Id.*

bidding presents potential concerns," including but not limited to:

a. "incentiviz[ing] invasive data-sharing by "push[ing] publishers [i.e. Defendant] to share as much end-user data as possible to get higher valuation for their ad inventory – particularly their location data and cookie cache, which can be used to ascertain a person's browsing history and behavior";

b. "send[ing] sensitive data across geographic borders;"

c. sending consumer data "to potentially dozens of bidders simultaneously, despite only one of those parties – the winning bidder – actually using that data to serve a targeted ad. Experts have previously cautioned that there are few (if any) technical controls ensuring [that] those other parties do not retain that data for use in unintended ways."[36]

83. Similarly, the Electronic privacy Information Center ("EPIC") has warned that consumers' privacy "is violated when entities disclose their information without authorization or in ways that thwart their expectations."[37]

84. Further, each of the three trackers embedded on Defendant's USA Today website ***re-installs its tracker cookies automatically every time a user visits the website.*** That happens even if the user previously had cleared the cookies from his or her web browser cache. As a result, USA Today website users, such as Plaintiffs and Class members, cannot escape the unauthorized sharing of their personally identifying and addressing information with third-parties Taboola, Amobee, and Xandr.

[36] Federal Trade Commission, Unpacking Real Time Bidding Through FTC's Case On Mobilewalla (Dec. 3, 2024), https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2024/12/unpacking-real-time-bidding-through-ftcs-case-mobilewalla (last visited May 8, 2025).

[37] Sara Geoghegan, What is Real Time Bidding?, EPIC (Jan. 15, 2025), https://epic.org/what-is-real-time-bidding/ (last visited May 8, 2025).

KELLER GROVER LLP
1965 Market Street, San Francisco, CA 94103
Tel. 415.543.1305 | Fax 415.543.7861

KELLER GROVER LLP
1965 Market Street, San Francisco, CA 94103
Tel. 415.543.1305 | Fax 415.543.7861

**D. Plaintiffs and Class Members Did Not Consent To Defendant's Disclosure of Their Personally Identifying and Addressing Information, and They Have a Reasonable Expectation of Privacy in Their User Data.**

85. Defendant does not ask its USA Today website visitors, including Plaintiffs, whether they consent to having their personally identifying and addressing information disclosed to and used by third parties like Taboola, Amobee, and Xandr. When a website user accesses and enters the USA Today website, there is no pop-up window or other notification to inform users that Defendant is using website tracking technology or installing third-party tracker cookies.

86. Additionally, the third-party trackers are incorporated seamlessly – ***and, to users, invisibly*** – in the background on the USA Today website. That seamless and invisible incorporation gave and gives Plaintiffs and Class members no way of knowing that Defendant was collecting their personally identifying and addressing information, including their IP addresses and device fingerprints, and secretly sharing that information with undisclosed third parties.

87. Further, although the USA Today website does have a Privacy Policy containing some disclosures about how information is collected and shared, that policy can be viewed only after scrolling all the way through the website content to the very bottom of the webpage. ***Thus, Defendant's policies and notices would be seen, if at all, only long after the third-party trackers and cookies had been installed on users' web browsers*** - in other words, only after it was too late.

88. In addition to its hard-to-see location, the hyperlink to access the Privacy Policy is written in small, inconspicuous font and is listed among many other links at the bottom of the USA Today webpage.

89. Unlike first-party cookies that may be technologically necessary to enable a computer user to view a webpage, ***third-party tracker cookies are not necessary***. Moreover, they (1) simultaneously communicate information to an external server as a user navigates a website; (2) track users across devices, meaning that a user's actions on multiple devices all will be included in the information stored regarding that user; (3) are not easily disabled by users; and/or (4) ***create a record of all of the information that users provide to and/or receive from the website***.

90. Because they were unaware of Defendant's use of third-party trackers and tracking cookies, Plaintiffs and Class members could not and did not consent to the collection, storage, and

KELLER GROVER LLP
1965 Market Street, San Francisco, CA 94103
Tel. 415.543.1305 | Fax 415.543.7861

use of their personally identifying and addressing information by undisclosed third parties such as Taboola, Amobee, and Xandr.

91. Plaintiffs and Class members had and have a reasonable expectation of privacy in their interactions with the USA Today website and in their user data, especially their personally identifying and addressing information. That expectation is even more pronounced for Plaintiffs' and Class members' IP addresses, which contain geolocation data that can be used to identify, track, and target individuals in a very specific way.

92. Privacy studies, such as those conducted by the *Pew Research Center*, show that most Americans are concerned about how data is collected about them.[38] Those privacy polls also reflect that Americans consider one of the most important privacy rights to be the need for a customer's or other individual's affirmative consent before a company collects and shares data regarding that customer or other individual.

93. Indeed, according to *Consumer Reports*, more than 90% of Americans believe that more should be done to ensure that companies protect consumers' privacy. Further, nearly two thirds of Americans – 64% – believe that companies should be prohibited from sharing data with third parties, while 63% of Americans want a federal law requiring companies to obtain a consumer's permission before sharing the consumer's information. To that end, 60% of Americans believe that companies should be required to be more transparent about their privacy policies so that consumers can make more informed choices.[39]

94. Users act in a manner that is consistent with those preferences. During a rollout of new iPhone operating software, for example, ***94% of U.S. users who were asked for clear,***

---

[38] Brooke Auxier et al., *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, Pew Research Center (Nov. 15, 2019), https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/ (last visited May 8, 2025).

[39] Benjamin Moskowitz et al., *Privacy Front & Center: Meeting the Commercial Opportunity to Support Consumer Rights*, Consumer Reports in collaboration with Omidyar Network (Fall 2020), https://thedigitalstandard.org/downloads/CR_PrivacyFrontAndCenter_102020_vf.pdf (last visited May 8, 2025).

***affirmative consent before allowing companies to track them chose not to share their data.***[40]

95. Defendant's unauthorized (1) installation of third-party tracker cookies on Plaintiffs' and Class members' web browsers and (2) disclosure of Plaintiffs' and Class members' personally identifying and addressing information to undisclosed third parties, all without adequate notification to the individual and certainly without any consent, are invasions of Plaintiffs' and Class members' privacy.

96. Plaintiffs and Class members have suffered injuries and damages in the form of (i) invasion of privacy; (ii) statutory damages; (iii) the continued and ongoing risk to their personally identifying information that, once out, cannot be restored to its previous level of privacy; and (iv) the continued and ongoing risk of harassment, spam, and targeted advertisements enabled by the USA Today website.

## CLASS ACTION ALLEGATIONS

97. Plaintiffs bring this action under Rule 23 of the Federal Rules of Civil Procedure on behalf of themselves and a class (the "USA Today Website Class" or "the Class") defined as follows:

> All California residents who, while located within California at any time during the applicable limitations period preceding the original filing of the Complaint in this matter and through and including the date of resolution, accessed and viewed the USA Today website and had their IP addresses and/or browser and device/operating system or other personal data collected by and disclosed to the third-party trackers embedded in the USA Today website.

98. Excluded from the USA Today Website Class are website users who (i) registered for the USA Today smartphone application and/or (ii) subscribed to receive the USA Today eNewspaper. Employees of Defendant and employees of Defendant's parents, subsidiaries, and corporate affiliates also are excluded from the Class. Plaintiffs reserve the right to amend or modify the class definition and/or to add sub-classes or limitations to particular issues, where appropriate, based upon subsequently-discovered information.

---

[40] *See* Margaret Taylor, How Apple Screwed Facebook, Wired (May 19, 2021) https://www.wired.co.uk/article/apple-ios14-facebook (last visited May 8, 2025).

KELLER GROVER LLP
1965 Market Street, San Francisco, CA 94103
Tel. 415.543.1305 | Fax 415.543.7861

99. This action properly may be maintained as a class action under Rule 23 of the Federal Rules of Civil Procedure because (1) there is a well-defined community of interest in the litigation, (2) common questions of law and fact predominate over individual issues, and (3) the proposed Class is ascertainable.

**Numerosity**

100. The USA Today Website Class that Plaintiffs seek to represent contains numerous members and is clearly ascertainable including, without limitation, by using Defendant's records and/or third-party trackers' records to determine the size of the Class and to determine the identities of individual Class members.

101. Based on information and belief, the USA Today Website Class consists of at least 75 individuals. The Class is so numerous that joinder of all members is impracticable.

**Typicality**

102. Plaintiffs' claims are typical of the claims of all of the other members of the USA Today Website Class, as Plaintiffs now suffer and have suffered from the same violations of the law as other putative Class members. Plaintiffs' claims and the Class members' claims are based on the same legal theories and arise from the same unlawful conduct, resulting in the same injury to Plaintiffs and all of the other Class members.

**Adequacy**

103. Plaintiffs will fairly and adequately represent and protect the interests of the other members of the Class. Plaintiffs have retained competent counsel with substantial experience in prosecuting complex litigation and class actions. Plaintiffs and their counsel are committed to prosecuting this action vigorously on behalf of the USA Today Website Class members and have the financial resources to do so. Neither Plaintiffs nor their counsel have any interests that are adverse to those of the other USA Today Website Class members.

**Commonality and Predominance**

104. By its unlawful actions, Defendant has violated Plaintiffs' and the Class members' rights under the CDAFA, CIPA, the California Constitution, common law, and the UCL. The questions raised are, therefore, of common or general interest to the Class members, who have a

KELLER GROVER LLP
1965 Market Street, San Francisco, CA 94103
Tel. 415.543.1305 | Fax 415.543.7861

well-defined community of interest in the questions of law and fact presented in this Complaint.

105. This action involves common questions of law and fact that predominate over any questions affecting only individual Class members. Those common questions of law and fact include, without limitation, the following:

(a) Whether Plaintiffs and Class members had a reasonable expectation of privacy when they accessed and visited the USA Today website;

(b) Whether Defendant knowingly and without permission accessed Plaintiffs' and Class members' computers or computer systems;

(c) Whether Defendant knowingly and without permission altered, damaged, deleted, destroyed, or otherwise used any data from Plaintiffs' and Class members' computers or computer systems;

(d) Whether Defendant knowingly and without permission took, copied, or made use of any data from Plaintiffs' and Class members' computers or computer systems;

(e) Whether Defendant knowingly and without permission added, altered, damaged, deleted, or destroyed any data from Plaintiffs' and Class members' computers or computer systems;

(f) Whether Defendant knowingly introduced any computer contaminant into Plaintiffs' and Class members' computers, computer systems, and/or computer networks;

(g) Whether Plaintiffs and Class members had a reasonable expectation of privacy in their personally identifying and addressing information, including IP addresses, when they accessed and visited the USA Today website;

(h) Whether each of the third-party trackers embedded in the USA Today website is a "pen register" under California Penal Code § 638.50(b);

(i) Whether Defendant has or had a policy or practice of disclosing and sharing personally identifying and addressing information collected on the USA Today website including, without limitation, IP addresses and/or browser and device/operating system data, with third-party trackers and/or other third parties;

KELLER GROVER LLP
1965 Market Street, San Francisco, CA 94103
Tel. 415.543.1305 | Fax 415.543.7861

KELLER GROVER LLP
1965 Market Street, San Francisco, CA 94103
Tel. 415.543.1305 | Fax 415.543.7861

(j) Whether Defendant has or had a policy or practice of not disclosing to USA Today website users that it would collect and share their personally identifying and addressing information, including IP addresses and/or browser and device/operating system data, with third-party trackers and/or other third parties;

(k) Whether Defendant has or had a policy or practice of not obtaining USA Today website users' prior consent to collect and share personally identifying and addressing information, including IP addresses and/or browser and device/operating system data, with third-party trackers and/or other third parties;

(l) Whether Defendant sought or obtained a court order for its use of the third-party trackers;

(m) Whether Defendant's conduct invaded Plaintiffs' and Class members' privacy;

(n) Whether Defendant's acts and practices violate or violated California's Computer Data Access and Fraud Act, Cal. Penal Code § 502;

(o) Whether Defendant's acts and practices violate or violated the California Invasion of Privacy Act, Cal. Penal Code § 638.51(a);

(p) Whether Defendant's acts and practices violate or violated the California Constitution or individual rights arising under the California Constitution;

(q) Whether Defendant's acts and practices resulted in unjust enrichment to Defendant;

(r) Whether Defendant's acts and practices violated California Business & Professions Code §§ 17200, *et seq*.; and

(s) Whether Plaintiffs and Class members are entitled to actual, statutory, nominal, and/or other forms of damages, restitution, and other relief.

**Superiority**

106. A class action is superior to other available methods for the fair and efficient adjudication of this controversy because individual litigation of the claims of all of the members of the Class is impracticable and because questions of law and fact common to the USA Today Website Class predominate over any questions affecting only individual members of the Class. Even if every individual member of the Class could afford individual litigation, the court system

KELLER GROVER LLP
1965 Market Street, San Francisco, CA 94103
Tel. 415.543.1305 | Fax 415.543.7861

could not. It would be unduly burdensome to the courts if individual litigation of the numerous cases were to be required. Individualized litigation also would present the potential for varying, inconsistent or contradictory judgments and would magnify the delay and expense to all parties and to the court system resulting from multiple trials of the same factual issues. By contrast, the conduct of this action as a class action with respect to some or all of the issues will present fewer management difficulties, conserve the resources of the court system and the parties, and protect the rights of each member of the USA Today Website Class. Further, it will prevent the very real harm that would be suffered by numerous members of the putative Class who simply will be unable to enforce individual claims of this size on their own, and by Defendant's competitors, who will be placed at a competitive disadvantage as their punishment for obeying the law. Plaintiffs anticipate no difficulty in the management of this case as a class action.

107. The prosecution of separate actions by individual members of the USA Today Website Class would create a risk of adjudications with respect to them that would, as a practical matter, be dispositive of the interests of other members of the Class who are not parties to those adjudications or that would substantially impair or impede the ability of those non-party members of the Class to protect their interests.

108. The prosecution of individual actions by members of the USA Today Website Class also would run the risk of establishing inconsistent standards of conduct for Defendant.

**FIRST CAUSE OF ACTION**
**Violation of the California Computer Data Access and Fraud Act**
**(California Penal Code § 502)**

109. Plaintiffs incorporate each allegation set forth above as if fully set forth herein and further allege as follows.

110. The California Legislature enacted the CDAFA with the intent to "expand the degree of protection afforded to individuals, businesses, and governmental agencies from tampering, interference, damage, and unauthorized access to lawfully created computer data and computer systems." Cal. Penal Code § 502(a).

111. The Legislature further declared that "protection of the integrity of all types and forms of lawfully created computers, computer systems, and computer data is vital to the

protection of the privacy of individuals as well as to the well-being of financial institutions, business concerns, governmental agencies, and others within this state that lawfully utilize those computers, computer systems, and data." Cal. Penal Code § 502(a).

112. To effectuate that purpose, the CDAFA affords a private right of action to owners of computers, systems, networks, programs, and/or data who suffer damages or loss as a result of a violation of the Act. Cal. Penal Code § 502(e)(1). There is no quantitative threshold of damage to bring a claim, and there is no monetary threshold to qualify for CDAFA protection.

113. For purposes of the statute, several definitions were provided. The term "access" means to "gain entry to, instruct, cause input to, cause output from, cause data processing with, or communicate with, the logical, arithmetical, or memory function resources of a computer, computer system, or computer network." Cal. Penal Code § 502(b)(1).

114. The term "computer program or software" is defined as "a set of instructions or statements, and related data, that when executed in actual or modified form, cause a computer, computer system, or computer network to perform specified functions." Cal. Penal Code § 502(b)(3).

115. The term "computer system" refers to "a device or collection of devices, including support devices and excluding calculators that are not programmable and capable of being used in conjunction with external files, one or more of which contain computer programs, electronic instructions, input data, and output data, that performs functions, including but not limited to, logic, arithmetic, data storage and retrieval, communication, and control." Cal. Penal Code § 502(b)(5).

116. Plaintiffs' and Class members' web browsers used to access the USA Today website are "computer software," and the computers on which Plaintiffs and Class members used their web browsers constitute computers or "computer systems" within the scope of the CDAFA.

117. The statute also defines the term "data" broadly to mean a "representation of information, knowledge, facts, concepts, computer software, or computer programs or instructions." The statute further provides that data may be in "any form, in storage media, or as stored in the memory of the computer or in transit or presented on a display device." Cal. Penal Code § 502(b)(8).

KELLER GROVER LLP
1965 Market Street, San Francisco, CA 94103
Tel. 415.543.1305 | Fax 415.543.7861

KELLER GROVER LLP
1965 Market Street, San Francisco, CA 94103
Tel. 415.543.1305 | Fax 415.543.7861

118. The term "computer contaminant" refers to "any set of computer instructions that are designed to modify, damage, destroy, record, or transmit information within a computer, computer system, or computer network without the intent or permission of the owner of the information. They include, but are not limited to, a group of computer instructions commonly called viruses or worms, that are self-replicating or self-propagating and are designed to contaminate other computer programs or computer data, consume computer resources, modify, destroy, record, or transmit data, or in some other fashion usurp the normal operation of the computer, computer system, or computer network." Cal. Penal Code § 502(b)(12).

119. As discussed above, a website cookie, including a third-party tracker cookie, and an IP address both are "data" within the meaning of the statute.

120. The website cookies installed by the Taboola Tracker, Amobee Tracker, and Adnxs tracker also constitute a "contaminant" under the CDAFA because they are designed to, and do, self-propagate to contaminate USA Today users' computers, computer systems, and computer networks to record and transmit data that would not otherwise be transmitted.

121. The third-party tracker cookies and tracking technology used by Defendant usurp the normal operation of Plaintiffs' and Class members' computing devices because they supplant Plaintiffs' and Class members' choices in how those devices and their resources, including energy and memory resources, are used. For example, the trackers command USA Today website users' computing devices to act in ways that are contrary to what was intended by Plaintiffs and Class members, such as storing unauthorized tracking cookies on their web browsers and disclosing to unknown third parties their identifying and addressing information without users' knowledge or consent.

122. As described above in more detail in Paragraph 89, third-party tracker cookies are not necessary for any of Plaintiffs' or Class members' devices to communicate effectively with Defendant or the USA Today website.

123. Under California Penal Code § 502(c)(1), it is unlawful to knowingly access and without permission alter, damage, delete, destroy, or otherwise use any data, computer, computer system, or computer network in order to…wrongfully control or obtain money, property or data.

Cal. Penal Code § 502(c)(1).

124. The statute also makes it unlawful to knowingly access and without permission take, copy, or make use of any data from a computer, computer system, or computer network. Cal. Penal Code § 502(c)(2).

125. The CDAFA further prohibits any person from knowingly accessing and without permission adding, altering, damaging, or destroying any data, computer software, or computer programs that reside or exist internal or external to a computer, computer system, or computer network. Cal. Penal Code § 502(c)(4).

126. Under subsections (6) and (7) of Penal Code § 502(c), a person also may not knowingly and without permission (i) provide or assist in providing a means of accessing or (ii) access or cause to be accessed any computer, computer system, or computer network. Cal. Penal Code §§ 502(c)(6) and (7).

127. Under California Penal Code § 502(c)(8), it also is unlawful to knowingly introduce any computer contaminant into any computer, computer system, or computer network. Cal. Penal Code § 502(c)(8).

128. Based on Defendant's unauthorized installation and storage of third-party tracker cookies on Plaintiffs' and Class members' web browsers, as alleged above, Defendant knowingly accessed and without permission altered and used Plaintiffs' and Class members' data and computer systems in violation of Penal Code § 502(c)(1).

129. Similarly, the installation of those third-party tracker cookies violates subsection (c)(4) because Defendant added and altered data and computer software on Plaintiffs' and Class members' computers or computer systems. Cal. Penal Code § 502(c)(4).

130. By installing third-party tracker cookies, Defendant also knowingly and without permission provided those trackers a means of accessing and/or caused to be accessed Plaintiffs' and Class members' computers, computer systems, and/or computer networks in violation of Penal Code §§ 502(c)(6) and (7). Defendant's actions caused the data processing functions and networks of users' devices to redirect Plaintiffs' and Class members' data to the third-party trackers.

131. Further, Defendant's unauthorized collection and disclosure of Plaintiffs' and Class

KELLER GROVER LLP
1965 Market Street, San Francisco, CA 94103
Tel. 415.543.1305 | Fax 415.543.7861

members' personally identifying and addressing information to undisclosed third parties violate Penal Code § 502(c)(2) because Defendant took and made use of data, including IP addresses, browser and device data, and other personal information, from Plaintiffs' and Class members' computers, computer systems, or computer networks.

132. Defendant's installation of the third-party tracker cookies also violates subsection (c)(8) because Defendant knowingly introduced a computer contaminant into Plaintiffs' and Class members' computers, computer systems, or computer networks. Cal. Penal Code § 502(c)(8).

133. Defendant lacked permission to use and access Plaintiffs' and Class members' data, computers, computer systems, and computer networks in the manners described above and lacked permission to introduce the third-party trackers into USA Today website users' web browsers, all as evidenced by the following:

(a) When entering and accessing Defendant's USA Today website, there is no pop-up window or other notification to inform users that Defendant is using website tracking technology or installing third-party tracker cookies;

(b) The third-party trackers are incorporated seamlessly and invisibly in the background on Defendant's USA Today website, thereby giving Plaintiffs and Class members no way of knowing that Defendant was allowing and enabling those third-party trackers to collect their personally identifying information, IP addresses, and device fingerprints; and

(c) Defendant does not seek permission from USA Today website visitors or otherwise ask them whether they consent to having their personally identifying and addressing information disclosed to and used by undisclosed third parties like Taboola, Amobee, and Xandr.

134. Defendant's knowing conduct as described herein, including embedding and implementing third-party trackers on its USA Today website and installing third-party tracker cookies on USA Today website users' browsers without their knowledge or consent, violates the CDAFA.

135. Plaintiffs and Class members are residents of California and were the owners or

KELLER GROVER LLP
1965 Market Street, San Francisco, CA 94103
Tel. 415.543.1305 | Fax 415.543.7861

KELLER GROVER LLP
1965 Market Street, San Francisco, CA 94103
Tel. 415.543.1305 | Fax 415.543.7861

lessees of the computers, computer systems, computer networks, and data described herein. Plaintiffs and Class members used their computers, computer systems and/or computer networks in California. Defendant accessed or caused to be accessed Plaintiffs' and Class members' data and other personally identifying information from within California.

136. Case law has established that misappropriation of data that has financial value can state an economic injury under the CDAFA. *See Brown v. Google LLC*, 685 F. Supp. 3d 909, 939-940 (N.D. Cal. 2023) (citing *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 600 (9th Cir. 2020)). In *Brown*, the court recognized that browsing histories and similar data carry financial value and that an economic market for that data exists. *Id.*; *see also, supra,* ¶ 34 (identifying examples of services and research panels that offer individuals compensation for the tracking of their data).

137. The financial value of Plaintiffs' and Class members' personal data collected without authorization by the third-party trackers embedded on the USA Today website is evidenced by, among other things, that data's extensive collection and use by third parties for real-time bidding, IP targeted advertising and geomarketing.

138. Defendant was unjustly enriched by accessing, acquiring, taking, and using Plaintiffs' and Class members' data and computer systems without their permission or consent, and by using all of that identifying information, including their IP addresses and browsing data, to maximize revenue from selling advertising space on the USA Today website and for Defendant's own financial benefit. Defendant has been unjustly enriched in an amount to be determined at trial.

139. Further, website tracking technology, such as tracking beacons and the third-party tracking cookies used by Defendant, take up and use processing, storage, and power resources to run on users' devices.[41] Those website tracking cookies also cause webpages to load more slowly,

[41] See Joshua M. Pearce, *Energy Conservation with Open Source Ad Blockers* (Mar. 30, 2020), https://www.mdpi.com/2227-7080/8/2/18 (last visited May 8, 2025); Computer Cookies: What They Are and How They Work, HP, https://www.hp.com/us-en/shop/tech-takes/what-are-computer-cookies (last visited May 8, 2025) ("Deleting cookies periodically can help protect your privacy by removing tracking data and free up storage space on your computer.").

KELLER GROVER LLP
1965 Market Street, San Francisco, CA 94103
Tel. 415.543.1305 | Fax 415.543.7861

thereby increasing the time and energy needed for devices to be used and to run. Overall, that additional processing, storage, and power usage results in increased energy and device costs for users. That extra cost is economic harm to Plaintiffs and Class members.

140. As a direct and proximate result of Defendant's violations of the CDAFA, Plaintiffs and Class members have suffered economic loss and damages. The statute imposes no minimum threshold for damages. Under Penal Code § 502(e)(1), Plaintiffs and Class members therefore are entitled to compensatory damages, injunctive relief, and other equitable relief in an amount to be determined at trial.

141. Plaintiffs and Class members also are entitled to an award of reasonable attorneys' fees and costs under Penal Code § 502(e)(2).

**SECOND CAUSE OF ACTION**
**Unlawful Use of a Pen Register or Trap and Trace Device**
**(California Penal Code § 638.51)**

142. Plaintiffs incorporate each allegation set forth above as if fully set forth herein and further allege as follows.

143. The California Legislature enacted the California Invasion of Privacy Act, Cal. Penal Code §§ 630, *et seq*. ("CIPA"), to address "advances in science and technology [that] have led to the development of new devices and techniques for the purpose of eavesdropping upon private communications" and declared "that the invasion of privacy resulting from the continual and increasing use of such devices and techniques has created a serious threat to the free exercise of personal liberties and cannot be tolerated in a free and civilized society." *Id*. § 630. CIPA is intended "to protect the right of privacy of the people of this state." *Id*.

144. Although CIPA was enacted before the dawn of the Internet, the California Supreme Court "regularly reads statutes to apply to new technologies where such a reading would not conflict with the statutory scheme." *In re Google Inc.*, 2013 WL 5423918, at *21 (N.D. Cal. Sept. 26, 2013); *see also Greenley*, 2023 WL 4833466, at *15 (***referencing CIPA's "expansive language" when finding that software was a "pen register"***); *Javier v. Assurance IQ, LLC*, 2022 WL 1744107, at *1 (9th Cir. May 31, 2022) ("Though written in terms of wiretapping, [CIPA] Section 631(a) applies to Internet communications."). This is consistent with the observation in

*Matera v. Google Inc.* that, "when faced with two possible interpretations of CIPA, the California Supreme Court has construed CIPA in accordance with the interpretation that provides the greatest privacy protection." *Matera v. Google Inc.*, 2016 WL 8200619, at *19 (N.D. Cal. Aug. 12, 2016).

145. Particularly pertinent here, California Penal Code § 638.51(a) makes it unlawful for a person to "install or use a pen register or a trap and trace device without first obtaining a court order."

146. A "pen register" is "a device or process that records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, but not the contents of a communication." Cal. Penal Code § 638.50(b).

147. A "trap and trace device" is a "a device or process that captures the incoming electronic or other impulses that identify the originating number or other dialing, routing, addressing, or signaling information reasonably likely to identify the source of a wire or electronic communication, but not the contents of a communication." Cal. Penal Code § 638.50(c).

148. In essence, a "pen register" is a "device or process" that records *outgoing* information, while a "trap and trace device" is a "device or process" that records *incoming* information. For example, if a user sends an email, a "pen register" might record the email address from which the email was sent, the email address to which the email was sent, and the subject line – because this is the user's *outgoing* information. On the other hand, if that same user receives an email, a "trap and trace device" might record the email address from which that email was sent, the email address to which it was sent, and the subject line – because this is *incoming* information that is being sent to that same user.

149. The three trackers embedded in the USA Today website – Taboola, Amobee, and Adnxs – are "pen registers" because each of them is a device or process that captures and records outgoing addressing or signaling information from the electronic communications transmitted by Plaintiffs' and Class members' computers, computer systems, and computer networks as they are accessing and visiting the USA Today website.

150. At all relevant times, Defendant installed and is installing each of the three pen

KELLER GROVER LLP
1965 Market Street, San Francisco, CA 94103
Tel. 415.543.1305 | Fax 415.543.7861

register trackers on Plaintiffs' and Class members' web browsers in California and used the trackers to collect Plaintiffs' and Class members' outgoing IP addresses and/or browser and device/operating system data.

151. Public IP addresses constitute addressing information because they disclose the general geographic coordinates of the user who is accessing and communicating with a website, but do not necessarily reveal any more about the underlying contents of the communication. *In re Zynga Privacy Litig.*, 750 F.3d 1098, 1108 (9th Cir. 2014).

152. Public IP addresses also constitute "routing" or "signaling" information because they are sending or directing users' communications from the routers in their homes or workplaces to the websites with which users are communicating.

153. Unaware of Defendant's installation and use of the third-party trackers as pen registers, Plaintiffs and Class members could not have provided and did not provide their prior consent to Defendant's installation or use of the third-party trackers or pen registers.

154. Upon information and belief, Defendant was not authorized by any court order to use a pen register to track Plaintiffs' and Class members' location data and other identifying or addressing information.

155. Defendant's conduct as described above violated California Penal Code § 638.51. As a result, Defendant is liable for the relief sought by Plaintiffs and the USA Today Website Class. Under California Penal Code § 637.2, Plaintiffs and Class Members are entitled to and seek statutory damages of $5,000 for each of Defendant's numerous CIPA violations.

**THIRD CAUSE OF ACTION**
**Invasion of Privacy**
**(Violation of Art. 1, § 1, California Constitution)**

156. Plaintiffs incorporate each allegation set forth above as if fully set forth herein and further allege as follows.

157. "Privacy" is listed in Article I, Section 1, of the California Constitution as a fundamental right of all Californians. That section of the Constitution provides as follows: "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and

KELLER GROVER LLP
1965 Market Street, San Francisco, CA 94103
Tel. 415.543.1305 | Fax 415.543.7861

obtaining safety, happiness, and privacy." Cal. Const. art. I, § 1.

158. The right to privacy in California's Constitution creates a right of action against private entities such as Defendant. To state a claim for invasion of privacy under the California Constitution, a plaintiff must establish (1) a legally protected privacy interest; (2) a reasonable expectation of privacy; and (3) an intrusion so serious in nature, scope, and actual or potential impact as to constitute an egregious breach of social norms.

159. Plaintiffs and Class members have a legally protected privacy interest in their personally identifying information and addressing information that are captured, without notice or consent, when they access and view the USA Today website. These privacy interests are recognized by the California Constitution, CDAFA, CIPA, HIPAA, and numerous other statutes.

160. Plaintiffs and Class members had a reasonable expectation of privacy under the circumstances, as they could not reasonably have expected that Defendant would violate state and federal privacy laws. Plaintiffs and Class members were not aware of and could not reasonably have expected that Defendant would use website tracking technology and install third-party tracker cookies without notice or without obtaining consent. Those unauthorized trackers collected and transmitted to undisclosed third parties Plaintiffs' and Class members' personally identifying and addressing information, including their device fingerprints and IP addresses, which contain geolocation data. This tracking resulted in pervasive and intrusive surveillance of users, such as Plaintiffs and Class members, over time and in defiance of their expectation of privacy.

161. Defendant's unauthorized (1) installation of third-party tracker cookies and (2) disclosure to and sharing with unknown third parties of Plaintiffs' and Class members' personally identifying and addressing information, all without consent or adequate notification to Plaintiffs and Class members, are invasions of Plaintiffs' and Class members' privacy.

162. Defendant's conduct constituted a serious invasion of privacy that would be highly offensive to a reasonable person in that (i) the information disclosed by Defendant and shared with third-party trackers was personally identifying information protected by the California Constitution and numerous California and federal statutes; (ii) Defendant did not have authorization or consent to disclose that personally identifying and addressing information,

KELLER GROVER LLP
1965 Market Street, San Francisco, CA 94103
Tel. 415.543.1305 | Fax 415.543.7861

including IP addresses and device fingerprints, to any third-party tracker embedded in the USA Today website, and the trackers did not have authorization to collect and use that sensitive and geolocation information; and (iii) the invasion deprived Plaintiffs and Class members of the ability to control the dissemination, circulation, and sale of that information, an ability that is a fundamental privacy right. Defendant's conduct constitutes a severe and egregious breach of social norms.

163. As a direct and proximate result of Defendant's actions, Plaintiffs and Class members have had their privacy invaded and have sustained injury, including injury to their peace of mind.

164. Plaintiffs and USA Today Website Class members seek appropriate relief for that injury, including but not limited to restitution, disgorgement of profits earned by Defendant because of, by way of, or in connection with the intrusions upon Plaintiffs' and Class members' privacy, nominal damages, and all other equitable relief that will compensate Plaintiffs and Class members properly for the harm to their privacy interests.

165. Plaintiffs also seek such other relief as the Court may deem just and proper.

**FOURTH CAUSE OF ACTION**
**Unjust Enrichment**
**(On Behalf of Plaintiffs and the Class)**

166. Plaintiffs incorporate each allegation set forth above as if fully set forth herein and further allege as follows.

167. Defendant received benefits from Plaintiffs and Class members and unjustly retained those benefits at their expense.

168. Plaintiffs and Class members conferred a benefit upon Defendant in the form of valuable personal information and data that Defendant collected from Plaintiffs and Class members without authorization and proper compensation. Defendant has collected, disclosed, and otherwise misused that information for its own gain, providing Defendant with economic, intangible, and other benefits, including substantial monetary compensation from third parties that received Plaintiffs' and Class members' personal information and data.

169. Defendant unjustly retained those benefits at the expense of Plaintiffs and Class

KELLER GROVER LLP
1965 Market Street, San Francisco, CA 94103
Tel. 415.543.1305 | Fax 415.543.7861

members because Defendant's conduct damaged Plaintiffs and Class members, all without providing any commensurate compensation to Plaintiffs and Class members.

170. The benefits that Defendant derived from Plaintiffs and Class members rightly belong to Plaintiffs and Class members. It would be inequitable under unjust enrichment principles in California for Defendant to be permitted to retain any of the profit or other benefits that it derived from the unfair and unconscionable methods, acts, and trade practices alleged in this Complaint.

171. Defendant should be compelled to disgorge in a common fund for the benefit of Plaintiffs and Class members all unlawful or inequitable proceeds that Defendant received, together with such other relief as the Court may deem just and proper.

**FIFTH CAUSE OF ACTION**
**Violations of California's Unfair Competition Law**
**(Cal. Bus. & Prof. Code §§ 17200, *et seq*.)**
**(On Behalf of Plaintiffs and the Class)**

172. Plaintiffs incorporate each allegation set forth above as if fully set forth herein and further allege as follows.

173. California Business & Professions Code §§ 17200, *et seq*. (the "UCL") prohibit unfair competition in the form of any unlawful, unfair, deceptive or fraudulent business act or practice.

174. Defendant's business acts and practices are "unlawful" under the UCL because, as alleged above, Defendant violated the California Constitution, California common law, and other California statutes and causes of action described in this complaint.

175. Defendant's business acts and practices are "unfair" under the UCL. California has a strong public policy of protecting consumers' privacy interests, including protecting consumers' personal data. Defendant violated that public policy by, among other things, surreptitiously collecting, disclosing, and otherwise misusing Plaintiffs' and Class members' personal information and data without Plaintiffs' and Class members' consent. Defendant's conduct violates the policies underlying the statutes referenced in this Complaint.

176. Defendant's business acts and practices also are "unfair" in that they are immoral, unethical, oppressive, unscrupulous, and/or substantially injurious to consumers. The gravity of

KELLER GROVER LLP
1965 Market Street, San Francisco, CA 94103
Tel. 415.543.1305 | Fax 415.543.7861

the harm caused by Defendant secretly collecting, disclosing, and otherwise misusing Plaintiffs' and Class members' personal information and data is significant. Further, there is no corresponding benefit to Plaintiffs and Class members resulting from that conduct. Finally, because Plaintiffs and Class members were completely unaware of Defendant's conduct, they could not have avoided the harm that Defendant inflicted upon them.

177. Defendant's violations were and are willful, deceptive, unfair, and unconscionable.

178. Had Plaintiffs and Class members known that their information would be collected and otherwise misused for Defendant's own benefit, they would not have used Defendant's USA Today website.

179. Plaintiffs have suffered an economic injury, *i.e.*, a loss of money or property. Plaintiffs have alleged that their browser and device data and personally identifying and addressing information, including their IP addresses, were collected by the three trackers embedded on Defendant's website and were disseminated and/or sold to other undisclosed third parties in exchange for monetary compensation received by Defendant. Plaintiffs also have alleged that that personal information has tangible monetary value and that Plaintiffs and Class members were deprived of that value when their browser and device data and personally identifying and addressing information, including their IP addresses, were disseminated and/or sold to other undisclosed third parties. These allegations are sufficient to establish an economic injury under the UCL. *See Calhoun v. Google LLC*, 526 F. Supp. 3d 605, 636 (N.D. Cal. 2021) ("[T]he Ninth Circuit . . . ha[s] concluded that plaintiffs who suffered a loss of their personal information suffered economic injury and had [UCL statutory] standing."); *Fraley v. Facebook, Inc.*, 830 F. Supp. 2d 785, 810-812 (N.D. Cal. 2011) (allegations that Facebook used plaintiffs' Facebook profiles to endorse third-party products and services, without compensation, sufficed). Nor are Plaintiffs' UCL claims barred by Plaintiffs not having paid for Defendant's services. *See Fraley*, 830 F. Supp. 2d at 811 (alleged injury was cognizable even though "[i]t is undisputed that Plaintiffs did not pay for Facebook's services").

180. Plaintiffs and Class members have a property interest in their sensitive personal data. By surreptitiously disclosing and otherwise misusing Plaintiffs' and Class members'

KELLER GROVER LLP
1965 Market Street, San Francisco, CA 94103
Tel. 415.543.1305 | Fax 415.543.7861

information, Defendant has taken property from Plaintiffs and Class members without providing just compensation or, indeed, any compensation.

181. California Business & Professions Code § 17203 provides that the Court may restore to any person in interest any money or property which may have been acquired by means of unfair, deceptive, and fraudulent business acts and practices, and may order restitution by Defendant to Plaintiffs for the practices alleged in this complaint. Plaintiffs and Class members are entitled under California Business & Professions Code §§ 17203 and 17208 to restitution and restoration of all ill-gotten money and property belonging to Plaintiffs and the Class.

182. Plaintiffs also seek injunctive relief in the form of a permanent injunction enjoining Defendant's unlawful and unfair business activities and practices, including an injunction terminating all downstream distributions of Plaintiffs' and Class members' illegally-collected personal data. Plaintiffs additionally seek any and all other equitable relief that the Court deems proper.

183. Plaintiffs' success in this action will enforce important rights affecting the public interest and, in that regard, Plaintiffs sue on behalf of the proposed class as well as on behalf of themselves and the general public.

184. Plaintiffs take upon themselves the enforcement of these laws and lawful claims. There is a financial burden incurred in pursuing this action and it would be against the interests of justice to penalize Plaintiffs by forcing them to pay attorneys' fees from the recovery in this action. Therefore, an award of attorneys' fees is appropriate under California Code of Civil Procedure § 1021.5.

## PRAYER FOR RELIEF

**WHEREFORE**, Plaintiffs, on behalf of themselves and the members of the Class, seek the following relief:

a. An order certifying the USA Today Website Class, appointing Plaintiffs Ryan Wu, Saber Khamooshi, and John Deddeh as representatives of the USA Today Website Class, and appointing counsel for Plaintiffs as counsel for the USA Today Website Class;

KELLER GROVER LLP
1965 Market Street, San Francisco, CA 94103
Tel. 415.543.1305 | Fax 415.543.7861

b. An order enjoining Defendant from engaging in the acts and practices complained of in this complaint;

c. An order declaring that Defendant's actions, as described above, violated California Penal Code § 502;

d. An order declaring that Defendant's actions, as described above, violated California Penal Code § 638.51;

e. An order declaring that Defendant's actions, as described above, violated Art. 1, § 1 of the California Constitution;

f. An order declaring that Defendant's actions, as described above, violated California Business & Professions Code §§ 17200, *et seq.*;

g. A judgment for and award of compensatory damages or other equitable relief under California Penal Code § 502(e)(1) to Plaintiffs and each of the members of the USA Today Website Class;

h. For each violation of CIPA, a judgment for and award of statutory damages of $5,000 under California Penal Code § 637.2 to Plaintiffs and each of the members of the USA Today Website Class;

i. A judgment for and award of restitution, disgorgement of profits, and nominal damages to which Plaintiffs and all of the members of the USA Today Website Class are entitled by law;

j. Disgorgement of profits and restitution and restoration of all costs incurred, sums or property unlawfully withheld, and/or losses caused by the acts and practices that violated California Business & Professions Code §§ 17200, *et seq.*;

k. Payment of costs of the suit;

l. Payment of attorneys' fees under California Code of Civil Procedure § 1021.5 and Penal Code § 502(e)(2);

m. An award of pre- and post-judgment interest to the extent allowed by law; and

n. Such other and/or and further relief as the Court may deem proper.

KELLER GROVER LLP
1965 Market Street, San Francisco, CA 94103
Tel. 415.543.1305 | Fax 415.543.7861

Respectfully submitted,

Dated: May 12, 2025

**KELLER GROVER LLP**

By: /s/ *Eric A. Grover*
ERIC A. GROVER
*Attorneys for Plaintiffs*
Ryan Wu and Saber Khamooshi

**COHELAN KHOURY & SINGER**

By: s/ *Isam C. Khoury*
Isam C. Khoury, Esq.
Attorneys for Plaintiff John Deddeh

**KEEGAN & BAKER, LLP**

By: /s/ *Patrick N. Keegan*
Patrick N. Keegan, Esq.
Attorneys for Plaintiff John Deddeh

**JURY DEMAND**

Plaintiffs request a trial by jury of all claims that can be so tried.

Respectfully submitted,

Dated: May 12, 2025

**KELLER GROVER LLP**

By: */s/ Eric A. Grover*
ERIC A. GROVER
*Attorneys for Plaintiffs*
Ryan Wu and Saber Khamooshi

**COHELAN KHOURY & SINGER**

By: s/ *Isam C. Khoury*
Isam C. Khoury, Esq.
Attorneys for Plaintiff John Deddeh

**KEEGAN & BAKER, LLP**

By: /s/ *Patrick N. Keegan*
Patrick N. Keegan, Esq.
Attorneys for Plaintiff John Deddeh

KELLER GROVER LLP
1965 Market Street, San Francisco, CA 94103
Tel. 415.543.1305 | Fax 415.543.7861

**CIVIL LOCAL RULE 5-1(i)(3) ATTESTATION**

Pursuant to L.R.5-1, the filer of this document, Eric Grover, hereby attests that all other signatories listed, and on whose behalf this filing is submitted, concur in the filing's content and have authorized this filing.

Dated: May 12, 2025

**KELLER GROVER LLP**

By: */s/ Eric A. Grover*
ERIC A. GROVER
*Attorneys for Plaintiffs*
Ryan Wu and Saber Khamooshi

KELLER GROVER LLP
1965 Market Street, San Francisco, CA 94103
Tel. 415.543.1305 | Fax 415.543.7861